

08-14-00

08/11/00

PTO/SB/05 (4/98)  
Approved for use through 09/30/2000. OMB 0651-0032  
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE  
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Please type a plus sign (+) inside this box ➔ +

**UTILITY  
PATENT APPLICATION  
TRANSMITTAL**

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No. 042390.P9016

First Inventor or Application Identifier Ramanathan Ramanathan

Title METHOD AND APPARATUS FOR MONITORING ENCRYPTED

Express Mail Label No. EL03443848US

ADDRESS TO: Assistant Commissioner for Patents  
Box Patent Application  
Washington, DC 20231

**APPLICATION ELEMENTS**  
See MPEP chapter 600 concerning utility patent application contents

1. ☒ Fee Transmittal Form  
(Submit an original, and a duplicate for fee processing)

2. ☒ Specification [Total Pages 26]  
(preferred arrangement set forth below)

- Descriptive title of the invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the invention
- Brief Summary of the invention
- Brief Description of the Drawings (if filed)
- Detailed Description
- Claim(s)
- Abstract of the Disclosure

3. ☒ Drawing(s) (35 U.S.C. 113) [Total Sheets 6]

4. Oath or Declaration [Total Pages 3]

a. ☒ Newly executed (original copy)

b. ☐ Copy from a prior application (37 C.F.R. § 1.63(d))  
(for continuation/divisional with Box 16 completed)

i. ☐ **DELETION OF INVENTOR(S)**  
Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR §§ 1.63(d)(2) and 1.33(b).

5. ☐ Microfiche Computer Program (Appendix)

6. Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary)

a. ☐ Computer Readable Copy

b. ☐ Paper Copy (identical to computer copy)

c. ☐ Statement verifying identity of above copies

**ACCOMPANYING APPLICATION PARTS**

7. ☒ Assignment Papers (cover sheet & document(s))

8. ☐ 37 C.F.R. § 3.73(b) Statement (when there is an assignee) ☐ Power of Attorney

9. ☐ English Translation Document (if applicable)

10. ☐ Information Disclosure Statement (IDS)/PTO - 1449 ☐ Copies of IDS Citations

11. ☐ Preliminary Amendment

12. ☒ Return Receipt Postcard (MPEP 503)  
(Should be specifically itemized)

13. ☐ \*Small Entity Statement(s) ☐ Statement filed in prior application, Status still proper and desired

14. ☐ Certified Copy of Priority Document(s)  
(if foreign priority is claimed)

15. ☐ Other: \_\_\_\_\_

**\*NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).**

16. If a **CONTINUING APPLICATION**, check appropriate box, and supply the requisite information below and in a preliminary amendment:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: \_\_\_\_\_

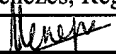
Prior application Information: Examiner \_\_\_\_\_ Group/Art Unit: \_\_\_\_\_

For **CONTINUATION** or **DIVISIONAL APPS** only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

**17. CORRESPONDENCE ADDRESS**

☐ Customer Number of Bar Code Label \_\_\_\_\_ (Insert Customer No. or Attach bar code label here) or ☒ Correspondence address below

Name	BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP					
Address	12400 Wilshire Boulevard, Seventh Floor					
City	Los Angeles	State	California	Zip Code	90025	
Country	U.S.A.	Telephone	(503) 684-6200	Fax	(503) 684-3245	

Name (Print/Type)	Clive D. Menezes, Reg. No. 45,493		
Signature		Date	08/11/00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

TITLE OF THE INVENTION

METHOD AND APPARATUS FOR MONITORING  
ENCRYPTED COMMUNICATIONS IN A NETWORK

INVENTOR

RAMANATHAN RAMANATHAN

Prepared by

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN  
12400 WILSHIRE BOULEVARD  
SEVENTH FLOOR  
LOS ANGELES, CA 90025-1026  
(503) 684-6200

Express Mail Label No. EL034438484US

042390.P9016

## COPYRIGHT NOTICE

Contained herein is material that is subject to copyright protection. The copyright  
5 owner has no objection to the facsimile reproduction of the patent disclosure by any  
person as it appears in the Patent and Trademark Office patent files or records, but  
otherwise reserves all rights to the copyright whatsoever.

## BACKGROUND OF THE INVENTION

### Field of the Invention

The present invention is related to the field of networking. In particular, the present  
invention is related to a method and apparatus for monitoring encrypted communications  
15 in a network.

### Description of the Related Art

Network security is a growing concern of organizations that employ networked  
computer systems. As a security measure, a corporation may wish to limit the  
communications between different groups of employees within the organization, or may  
20 desire to keep individuals from within the corporate structure from snooping in on the  
transmission of other employees within the corporation, or the corporation may wish to  
monitor the content of information that is transmitted between different employees within  
the corporate network.

A corporation may use a firewall to keep internal network segments secure and insulated from each other. For example, a research or accounting subnet might be vulnerable to snooping from within, and a firewall to prevent snooping may be employed.

5 A corporation may have in place a network policy (NP) as part of its security measures. A NP may include a communication scheme that defines which computers, or groups of computers are granted permission to communicate with each other, the type of encryption and authentication algorithms that are used by each computer, and the duration of time during which the encryption and authentication keys are valid. A NP may be installed on a policy server responsible for distributing and managing the NP on  
10 all network elements within its jurisdiction.

Traditionally a secret key such as the Data Encryption Standard (DES) standard that is well known in the art has been used to encrypt data. Figure 1 illustrates a network element 203 transmitting an email message, and another network element 204 receiving the transmitted message using the same key to encrypt and decrypt messages. However,  
15 transmitting the secret key to the recipient poses a problem because the method employed in transferring the key from the sender to the receiver may not be secure. Moreover, even if a secure method were available to transmit the secret key from network element 203 to network element 204, network monitoring element 202 would be unable to monitor the encrypted communications between because it would not be in possession of the key.

20 Alternatively, a corporation may use a public-key cryptography method, also well known in the art. This method uses both a private and a public key. Each recipient has a private key that is kept secret and a public key that is published. The sender looks up the recipient's public key and uses it to encrypt the message. The recipient uses the private

key to decrypt the message. Thus, the private keys are not transmitted and are thereby secure. In this method too, a network monitoring element such as a network administrator will be unable to monitor the encrypted communications between two computers on the network as the network monitoring element is not in possession of the

5 key that is needed to decrypt the data. The prior art fails to describe a method or an apparatus for monitoring encrypted communications in a network, by a network administrator or by a network element such as another computer that has the authority to do so.

042390.P9016

## BRIEF SUMMARY OF THE DRAWINGS

Figure. 1 illustrates an embodiment of a prior art system wherein data is encrypted.

Figure. 2 illustrates an embodiment of the disclosed invention using a policy server and a policy administrator to monitor encrypted communications in a network.

5 Figure. 3 is a flow diagram illustrating an overview of an embodiment of the invention.

Figure. 4 is a flow diagram of the communication process between network elements.

Figure. 5 is a flow diagram illustrating details of an embodiment of the invention.

Figure 6. illustrates a policy server comprising an embodiment of the invention.

10 Figure 7. illustrates a network monitoring element comprising an embodiment of the invention.

042390.P9016

DETAILED DESCRIPTION OF THE INVENTION

Described is a method and apparatus for monitoring encrypted communications in a network. In particular, the invention describes a method and apparatus for monitoring encrypted communications in a network comprising establishing a network policy (NP) on a policy server, establishing a network monitoring digital contract (NMDC) between the policy server and a network monitoring element, establishing a network use digital contract (NUDC) between the policy server and a first network element, establishing a NUDC between the policy server and a second network element, and monitoring communications between the first network element and the second network element, by the network monitoring element, in accordance with the network policy, the network monitoring digital contract, and network use digital contracts.

In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one of ordinary skill in the art that the present invention may be practiced without these specific details. In other instances, well-known architectures, steps, and techniques have not been shown to avoid unnecessarily obscuring the present invention. For example, specific details are not provided as to whether the method is implemented in local area network (LAN), a wide area network (WAN), or across the Internet. Also, specific details are not provided as to whether the method is implemented as a software routine, hardware circuit, firmware, or a combination thereof. While the description that follows addresses the method as it applies to a Local Area Network (LAN) application, it is appreciated by those of ordinary skill in the art that the method is generally applicable

to any network application including, but not limited to, internetworks (Internet), Metropolitan Area Networks (MANs), and Wide Area Networks (WANs).

In one embodiment, Figures 2 and 3 illustrate a network comprising a plurality of policy servers 201, a plurality of network monitoring elements 202, and network elements 203 and 204 (such as computers). At 300, a network policy (NP) is defined, distributed and administered by policy administrator 205. At 310 the policy administrator transmits the NP to each network element. A network element may only communicate with another network element in accordance with a particular communication rule defined in the NP. If two network elements are allowed to communicate with each other, the NP stipulates the type of encryption algorithm, authentication algorithm, the type of keys used for encryption and authentication, and the duration of time during which the keys are valid. The term network element as used here is generic and is to be construed to include any network element including computers, which may communicate with each other.

In 320, once the NP has been transmitted to each network element, a network monitoring element 202 that desires to monitor the communication between network elements 203 and 204, obtains a network monitoring digital contract (NMDC) from the policy administrator 205. Although the description that follows is for a network administrator to monitor communication between network elements, any network element that possesses the required authorization as indicated in the NP may monitor the communications between network elements. In one embodiment the policy administrator 205, and the network monitoring element 202, are physically located on the same device. In one embodiment, prior to issuing the NMDC, the policy administrator 205

authenticates the network administrator 202 by requesting from the network administrator its proof of identity. In one embodiment this proof of identity is a digital certificate. A digital certificate is the digital equivalent of an identity (ID) card used in conjunction with a public key encryption system. Digital certificates are well known in the art and are issued by third parties known as certification authorities (CAs) such as VeriSign, Inc., of Mountain View, CA. After receiving the digital certificate from the network administrator 202 and after authenticating the network administrator, the policy administrator 205 requests and receives from the network administrator 202 the network administrator's authorization, which in one embodiment is a legal corporate authorization. The network administrator's authorization or legal corporate authorization validates the network administrator's authority to monitor network communications as specified in the NP. The authorization, or legal corporate authorization comprises a digital signature. A digital signature is an electronic signature that is well known in the art. The policy administrator authenticates the network administrator's digital signature. On receiving and authenticating both, the digital certificate that authenticates the network administrator, as well as the digital signature that validates the network administrator's authority to monitor network communications, the policy administrator 205 issues the network monitoring element a NMDC. The NMDC includes the digital certificate of the policy administrator 205, the digital certificate of the network administrator 202, the digital signature of the network administrator 202, the digital signature of the policy administrator 205, the date, the time, and the content of the transaction. In one embodiment the content of the transaction includes the type of decrypting information to be transmitted, including the decrypting keys needed for decrypting the encrypted

communication between the communicating elements. The NMDC also includes the period during which the NMDC is valid. A copy of the NMDC is maintained on the policy administrator 205 prior to transmitting the NMDC to the network administrator 202. On receipt of the NMDC, the network administrator maintains a copy for future use.

5           The network administrator 202 transmits the NMDC to the policy administrator 205 each time the network administrator desires monitoring the communications between network elements. The policy administrator 205 verifies the validity of the NMDC and issues the network administrator the information it needs to decrypt the communication between the elements it intends to monitor. The aforementioned validation process is  
10       performed each time the network administrator desires monitoring the encrypted communications because the decryption keys could be different for each set of communicating elements. The network administrator has to renew its NMDC once the NMDC expires. The process to renew the NMDC is as explained above.

          In addition to the NMDC, at 330, a second digital contract called the network use  
15       digital contract (NUDC) is established between each network element and the policy administrator 205. In particular, each network element registers itself with the policy administrator 205 as one of the policy server's clients and agrees to be bound by the rules in the NP and the NUDC. The NUDC includes the digital certificate of the registering network element 203, the digital certificate of the policy administrator 205, the digital  
20       signature of the policy server, the digital signature of the network element, the date, the time, the content of the transaction, and the period during which the NUDC is valid. In one embodiment a copy of the NUDC is maintained on the policy server and on the network element. The NUDC is valid as long as the network element follows the rules

established by the NP and the NUDC. In one embodiment, if the network element chooses not to follow the established rules, a record of the infraction is maintained in its encryption and authentication log, a copy of the infraction is sent to the policy administrator, and the network element will not be able to communicate with other network elements on the network. In one embodiment, the content of the transaction in the NUDC includes establishing the authority for the policy administrator 205 to secretly access the encryption and authentication log and obtain the decryption information stored on the network element. Establishment of such authority may be performed using any one of a number of authorization techniques known in the art.

Referring to figure 4, after the NP, the NMDC and the NUDC are in place, at 400 a network element 203 desires to communicate with another network element 204, at 410 network element 203 looks up the NP it received from the policy administrator 205 to determine if it has the authority to communicate with network element 204. If the authority to communicate exists, at 420, network element 203 determines whether to communicate with network element 204 using the encryption and authentication rules of the NP or its own encryption and authentication algorithm. At 430, network element 203 having decided to use its own encryption and authentication algorithm, logs the details of the encryption and authentication algorithms including any keys needed to decrypt the communications between network elements 203 and 204. In one embodiment, the logs stored on network element 203 are stored in an encrypted format. At 440, network element 203 after logging the encryption and authentication algorithm it intends using, including the decrypting keys, communicates with network element 204 in an encrypted format. At 450, network element 203 logs the encryption and authentication algorithm

including the decrypting keys as specified by the NP. In one embodiment, the logs stored on the policy server are in an encrypted format. At 460, network element 203 uses the encryption and authenticating algorithm logged and communicates with network element 204.

5 Referring to figure 5, the process by which network administrator 202 monitors encrypted communications between network elements 203 and 204 will now be described. At 581, the NMDC and the NUDC have been established. At 500, network administrator 202 decides to monitor the communications between network elements 203 and 204. At 510, the policy administrator 205 receives the NMDC from the network  
10 administrator 202. At 520, the policy administrator 205 authenticates the NMDC. After determining that the NMDC is valid, at 540 the policy administrator determines whether it has the decrypting information in its own log. In one embodiment, decrypting information includes decrypting keys for decrypting the encrypted communications between the network elements. If the policy administrator has the decrypting  
15 information, at 560 the policy administrator transmits the decrypting information to network administrator 202. At 590, the network administrator uses the decrypting information obtained from the policy administrator to decrypt the encrypted communications between network elements 203 and 204. At 550, if policy administrator does not have the decrypting information in its log, it obtains the decrypting information  
20 from the log on network elements 203 or 204 and transmits the decrypting information to the network administrator 202. In another embodiment, at 580, policy administrator 202 decrypts the communication between network elements 203 and 204 and transmits the

information to network administrator 202. This transfer of information is done via a secure link between the policy administrator 205 and the network administrator 202.

Figure 6 illustrates an apparatus of an embodiment of the invention. In particular, figure 6 illustrates a policy server in which an embodiment of the invention is employed.

5 The apparatus comprises a receiver 600 to receive an NMDC from a network monitoring element and to receive a request for decrypting communications between network elements. Communicatively coupled to the receiver is a microprocessor 610 with a memory 620. The microprocessor 610 authenticates the NMDC and retrieves decrypting information either from memory 620 or from network elements. Communicatively  
10 coupled to the microprocessor 610 is a transmitter 630 for transmitting the initial copy of the NMDC to the network monitoring element, for transmitting a copy of the NUDC to a network element, and for transmitting decrypting information, including decrypting keys that are used by the network monitoring element to decrypt the encrypted communications between network elements. In one embodiment the microprocessor  
15 reads the logs containing the decrypting information on a network element, and obtains the decrypting keys, decrypts the communication between network elements and the transmitter transmits the decrypted communications to the network monitoring element.

Figure 7 illustrates an apparatus of an embodiment of the invention. In particular, figure 7 illustrates a network monitoring element in which an embodiment of the  
20 invention is employed. The apparatus comprises a receiver 700 to initially receive the NMDC from the policy administrator, and to subsequently receive decrypting information, including decrypting keys to decrypt the encrypted communication it receives between network elements. In one embodiment the receiver 700 receives the

decrypted communications between network elements from the policy administrator.

Communicatively coupled to the receiver 700 is a microprocessor 710 and a memory 720. The microprocessor uses the decrypting keys obtained from the policy administrator and decrypts the encrypted communication between network elements. The memory 720

5 stores a copy of the NMDC that the apparatus receives from the policy administrator.

Communicatively coupled to the microprocessor and memory is a transmitter 730. The transmitter transmits a request to monitor encrypted communications between network elements, and then transmits the NMDC that is stored in memory 720 to the policy administrator.

10 Thus a method has been disclosed for monitoring encrypted communications in a network environment. Embodiments of the invention may be represented as a software product stored on a machine-readable medium (also referred to as a computer-readable medium or a processor-readable medium). The machine-readable medium may be any type of magnetic, optical, or electrical storage medium including a diskette, CD-ROM,  
15 memory device (volatile or non-volatile), or similar storage mechanism. The machine-readable medium may contain various sets of instructions, code sequences, configuration information, or other data. For example, the procedures described herein for polling network elements by network management stations can be stored on the machine-readable medium. Those of ordinary skill in the art will appreciate that other instructions  
20 and operations necessary to implement the described invention may also be stored on the machine-readable medium.

CLAIMS

What is claimed is:

- 5           1. A method comprising a policy administrator:
- establishing a network monitoring digital contract with a network monitoring
- element;
- establishing a network use digital contract with a first and a second network
- element; and
- 10           transmitting decrypting information to the network monitoring element for
- decrypting encrypted communications between the first network element and the
- second network element per terms in the network monitoring digital contract and
- the network use digital contract.
- 15           2. The method of claim 1, wherein transmitting decrypting information to the
- network monitoring element for decrypting encrypted communications between
- the first network element and the second network element per terms in the
- network monitoring digital contract and the network use digital contract
- comprises the policy administrator:
- 20           receiving a request from the network monitoring element for the decrypting
- information;
- transmitting a request to the network monitoring element for the network
- monitoring digital contract;

receiving the network monitoring digital contract from the network monitoring element;

authenticating the received network monitoring digital contract; and

transmitting decrypting keys to decrypt the encrypted communications between

the first network element and the second network element to the network monitoring element.

3. The method of claim 1, wherein transmitting decrypting information to the network monitoring element for decrypting encrypted communications between the first network element and the second network element per terms in the network monitoring digital contract and the network use digital contract comprises the policy administrator decrypting the encrypted communications between the network elements and transmitting the decrypted communications to the network monitoring element.

4. The method of claim 1, wherein establishing a network monitoring digital contract with a network monitoring element comprises:

receiving a network monitoring element's digital certificate;

authenticating the network monitoring element's digital certificate;

receiving a network monitoring element's digital signature;

authenticating the network monitoring element's digital signature;

writing contract terms in an electronic document;

writing the network monitoring element's digital certificate and the network monitoring element's digital signature in the electronic document;  
writing a digital certificate of the policy administrator and a digital signature of the policy administrator in the electronic document; and  
5 transmitting a copy of the electronic document to the network monitoring element.

5. The method of claim 4, wherein writing contract terms in an electronic document comprises:

10 writing an effective date and time of the network monitoring digital contract;  
writing a time period during which the network monitoring digital contract is valid; and  
specifying the decrypting information, including decrypting keys the network monitoring element is to receive.

- 15 6. The method of claim 1, wherein establishing a network use digital contract with each network element comprises:

receiving a network element's digital certificate;  
authenticating the network element's digital certificate;  
20 receiving a network element's digital signature;  
authenticating the network element's digital signature;  
writing contract terms in an electronic document;

writing the network element's digital certificate and the network element's digital signature in the electronic document;

writing a digital certificate of the policy administrator and a digital signature of the policy administrator in the electronic document; and

5 transmitting a copy of the electronic document to the network element.

7. The method of claim 6, wherein writing contract terms in an electronic document comprises:

writing an effective date and time of the network use digital contract; and

10 specifying the decrypting information, including decrypting keys the policy administrator obtains from the network element.

8. The method of claim 1 further comprising:

establishing a network policy; and

15 transmitting the network policy to network elements.

9. A method, comprising a network monitoring element:

establishing a network monitoring digital contract with a policy administrator;

20 transmitting a request to monitor encrypted communications between network elements;

transmitting the network monitoring digital contract; and

receiving decrypting information, including decrypting keys from the policy administrator for decrypting encrypted communications between a first network

element and a second network element per the terms in the network monitoring digital contract.

5 10. The method of claim 9, wherein receiving decrypting information from the policy administrator for decrypting encrypted communications between a first network element and a second network element per the terms in the network monitoring digital contract comprises receiving from the policy administrator decrypted communications after the policy administrator decrypts the encrypted

10 communications between the network elements.

11. The method of claim 9, wherein establishing a network monitoring digital contract with a policy administrator comprises a network monitoring element: transmitting its digital certificate to the policy administrator;

15 transmitting its digital signature to the policy administrator; and receiving a copy of the network monitoring digital contract from the policy administrator.

12. A method, comprising:

20 establishing by a first network element, a network use digital contract with a policy administrator;

communicating with a second network element per the terms of the network use digital contract;

logging in a secure manner, encryption and authenticating algorithms, and decryption keys used in the communication; and permitting the policy administrator access to the log to obtain the decrypting keys.

- 5 13. The method of claim 12, wherein establishing by a first network element, a network use digital contract with a policy administrator comprises a network element:
- transmitting its digital certificate;
- transmitting its digital signature; and
- 10 receiving a copy of the network use digital contract from the policy administrator.

14. An article of manufacture comprising:
- a machine-readable medium that provides instructions, that when executed by a machine, cause said machine to perform operations comprising:
- 15 establishing a network monitoring digital contract with a network monitoring element;
- establishing a network use digital contract with a first and a second network element; and
- transmitting decrypting information to the network monitoring element for
- 20 decrypting encrypted communications between the first network element and the second network element per terms in the network monitoring digital contract and the network use digital contract.

15. The machine-readable medium of claim 14, wherein said instructions for transmitting decrypting information to the network monitoring element for decrypting encrypted communications between the first network element and the second network element per terms in the network monitoring digital contract and the network use digital contract, include further instructions to direct the policy administrator to receive a request from the network monitoring element for the decrypting information; to receive the network monitoring digital contract from the network monitoring element; to authenticate the network monitoring digital contract; and to transmit decrypting information, including decrypting keys needed to decrypt the encrypted communications between the network elements.

16. The machine-readable medium of claim 14, wherein said instructions for transmitting decrypting information to the network monitoring element for decrypting encrypted communications between the first network element and the second network element per terms in the network monitoring digital contract and the network use digital contract include further instructions to decrypt the encrypted communications between the network elements; and to transmit the decrypted communications to the network monitoring element.

17. The machine-readable medium of claim 14, wherein said instructions establishing a network monitoring digital contract between a policy administrator and a network monitoring element include further instructions to receive a network monitoring element's digital certificate and digital signature; to authenticate the

network monitoring element's digital certificate and digital signature; to write the contract terms, including an effective date and time of the network monitoring digital contract; to specify a time period during which the network monitoring digital contract is valid; to specify the decrypting information, including  
5 decrypting keys the network monitoring element is to obtain in an electronic document; to write the network monitoring element's digital certificate and digital signature in the electronic document; to write a digital certificate and a digital signature of the policy administrator in the electronic document; and to transmit a copy of the electronic document to the network monitoring element.

10

18. The machine-readable medium of claim 14, wherein said instructions establishing a network use digital contract between the policy administrator and network elements include further instructions to receive a network element's digital  
certificate and digital signature; to authenticate the network elements digital  
15 certificate and digital signature; to write contract terms, including an effective date and time of the network use digital contract; to specify the decrypting information, including decrypting keys the policy administrator is to obtain in an electronic document; to write the network element's digital certificate and digital signature in the electronic document; to write a digital certificate and a digital  
20 signature of the policy administrator in the electronic document; and to transmit a copy of the electronic document to the network element.

19. The machine-readable medium of claim 14, wherein said instructions include further instructions to establish a network policy; and to transmit the network policy to network elements.

20. An article of manufacture comprising:

a machine-readable medium that provides instructions, that when executed by a machine, cause said machine to perform operations comprising:

establishing a network monitoring digital contract with a policy administrator;

transmitting a request to monitor encrypted communications between network elements;

transmitting the network monitoring digital contract; and

receiving decrypting information, including decrypting keys from the policy administrator for decrypting encrypted communications between a first network element and a second network element per the terms in the network monitoring digital contract.

21. The machine-readable medium of claim 20, wherein said instructions for

receiving decrypting information from the policy administrator for decrypting encrypted communications between a first network element and a second network element per the terms in the network monitoring digital contract include further instructions to receive from the policy administrator decrypted communications after the policy administrator decrypts the encrypted communications between the network elements.

22. The machine-readable medium of claim 20, wherein said instructions for  
establishing a network monitoring digital contract with a policy administrator  
include further instructions for a network monitoring element to transmit its  
digital certificate to the policy administrator; to transmit its digital signature to the  
5 policy administrator; and to receive a copy of the network monitoring digital  
contract from the policy administrator.

23. An article of manufacture comprising:

a machine-readable medium that provides instructions, that when executed by a  
10 machine, cause said machine to perform operations comprising:  
establishing by a first network element, a network use digital contract with a  
policy administrator;  
communicating with a second network element per the terms of the network use  
digital contract;  
15 logging in a secure manner, encryption and authenticating algorithms, and  
decryption keys used in the communication; and  
permitting the policy administrator access to the log to obtain the decrypting keys.

24. The machine-readable medium of claim 23, wherein said instructions for  
20 establishing by a first network element, a network use digital contract with a  
policy administrator include further instructions for a network element to transmit  
its digital certificate; to transmit its digital signature; and to receive a copy of the  
network use digital contract from the policy administrator.

25. An apparatus comprising:

a receiver to receive a request for decrypting information, and to receive a  
network monitoring digital contract from a network monitoring element;  
5 a microprocessor communicatively coupled to said receiver and a memory, to  
authenticate the network monitoring digital contract; and  
a transmitter communicatively coupled to said microprocessor and memory to  
transmit a network policy and decrypting information, including decrypting keys  
to decrypt encrypted communications between network elements.

10 26. The apparatus of claim 25, wherein the microprocessor retrieves from the memory  
decrypting information including decrypting keys, to decrypt the encrypted  
communications between the network elements and to transmit the decrypted  
communications to the network monitoring element.

15 27. The apparatus of claim 25, wherein the microprocessor retrieves from a network  
element decrypting information including decrypting keys and the transmitter  
transmits the decrypting information to the network monitoring element.

20 28. An apparatus comprising:

a receiver to receive a network monitoring digital contract, and decrypting  
information, including decrypting keys from a policy administrator;

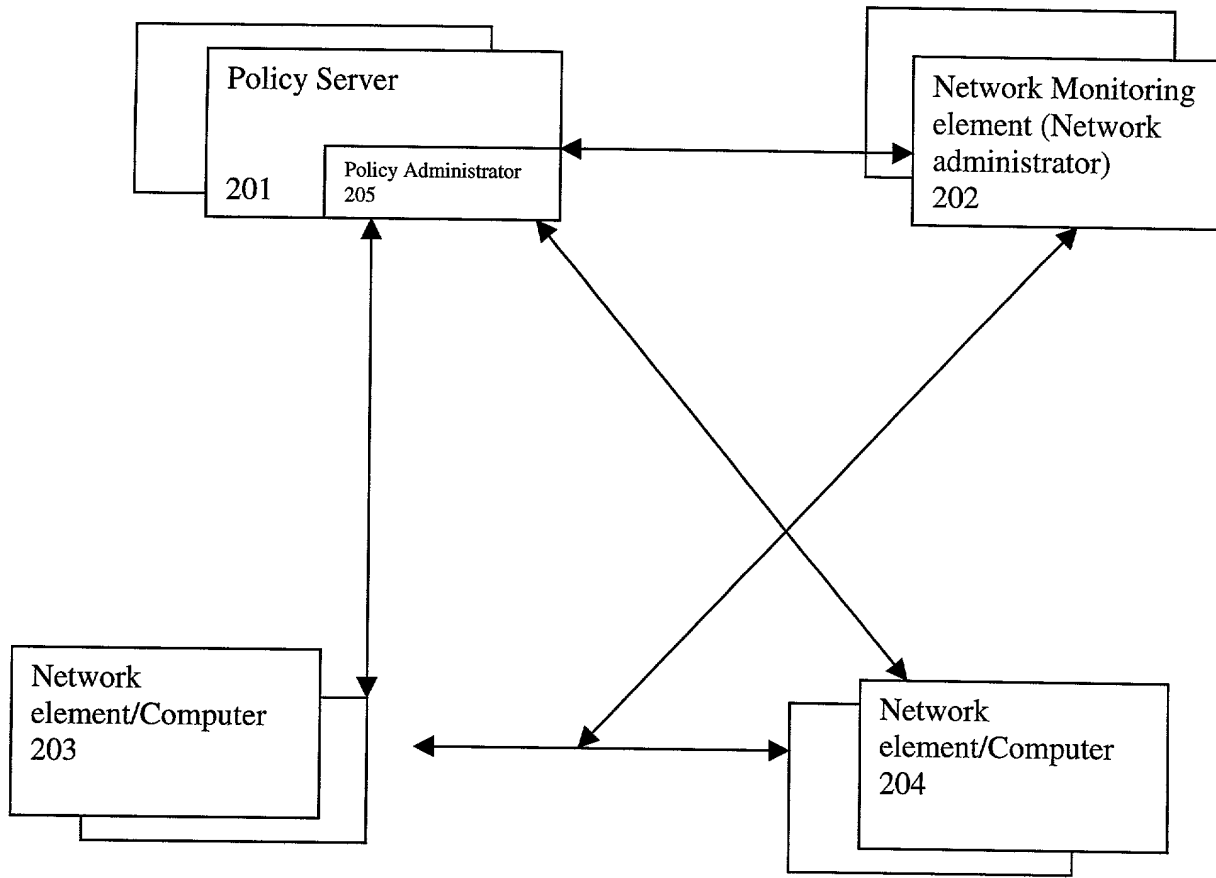
said receiver to receive encrypted communications between a first network  
element and a second network element;  
a microprocessor communicatively coupled to the receiver and a memory, said  
memory to store the network monitoring digital contract, and to use the  
5 decrypting information, including the decrypting keys to decrypt the encrypted  
communications between the first and the second network element;  
a transmitter communicatively coupled to the microprocessor and the memory to  
transmit a request to the policy administrator for the decrypting information,  
including the decrypting keys to decrypt the encrypted communications between  
10 the first and the second network element, and to transmit the network monitoring  
digital contract to the policy administrator.

29. The apparatus of claim 28, wherein the receiver receives decrypted  
communications from the policy administrator.

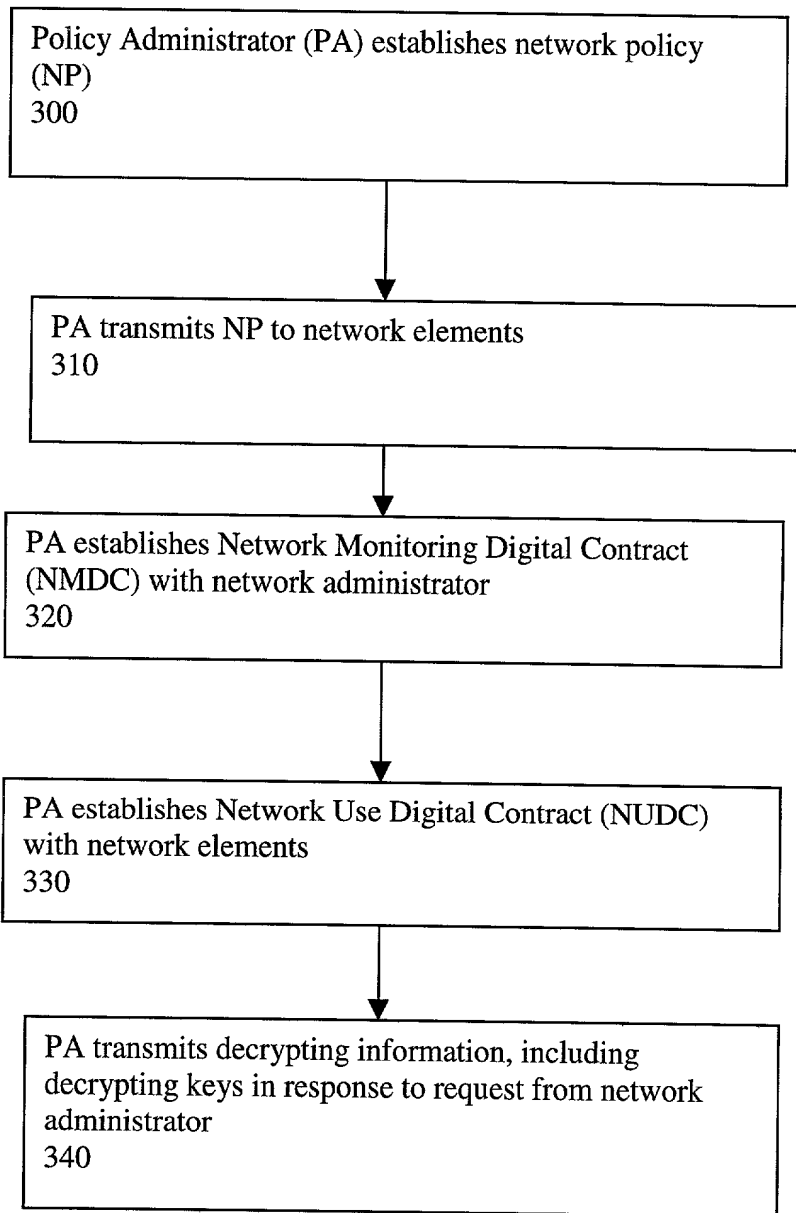
## 10

5





**Figure 2**



**Figure 3**

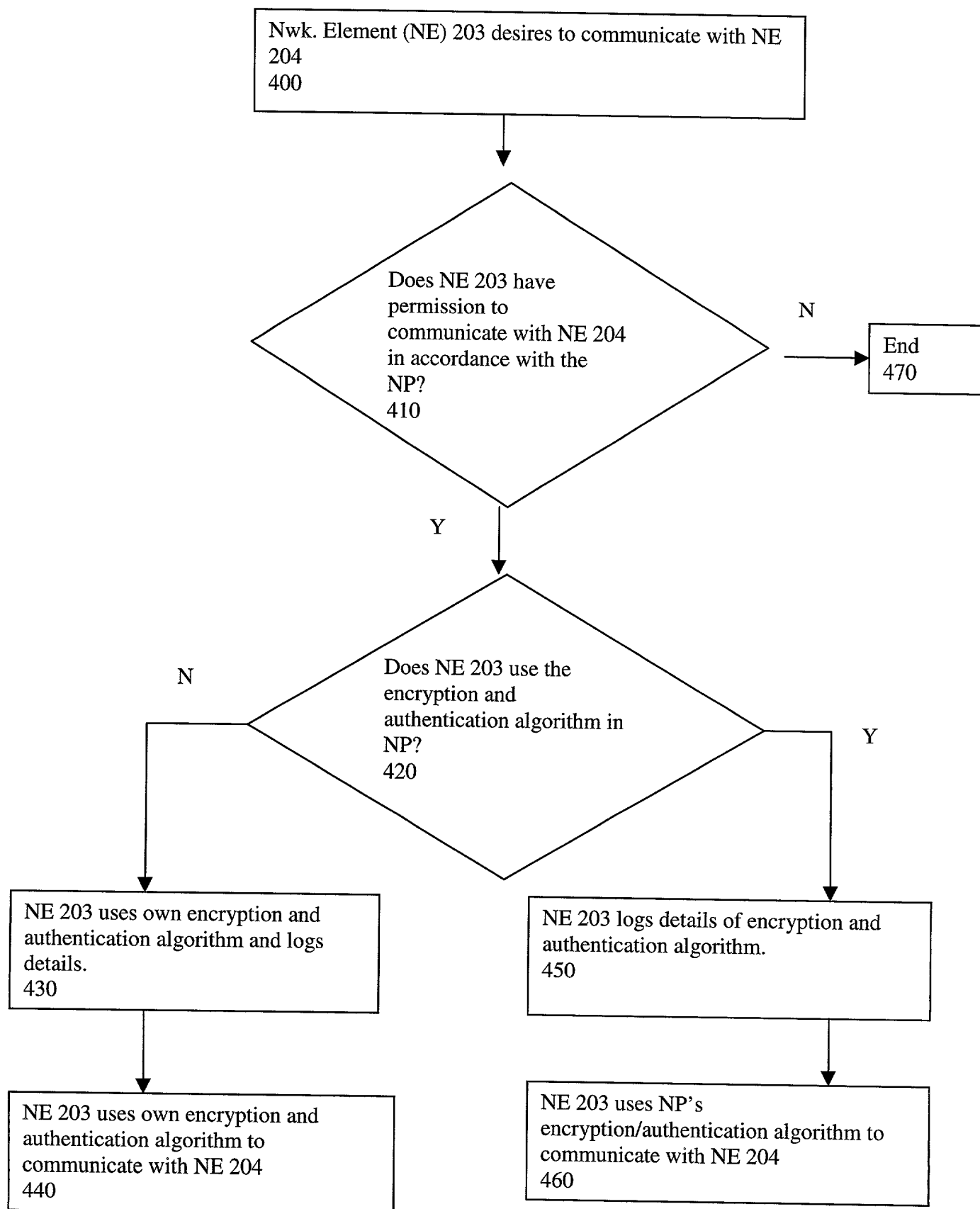


Figure 4

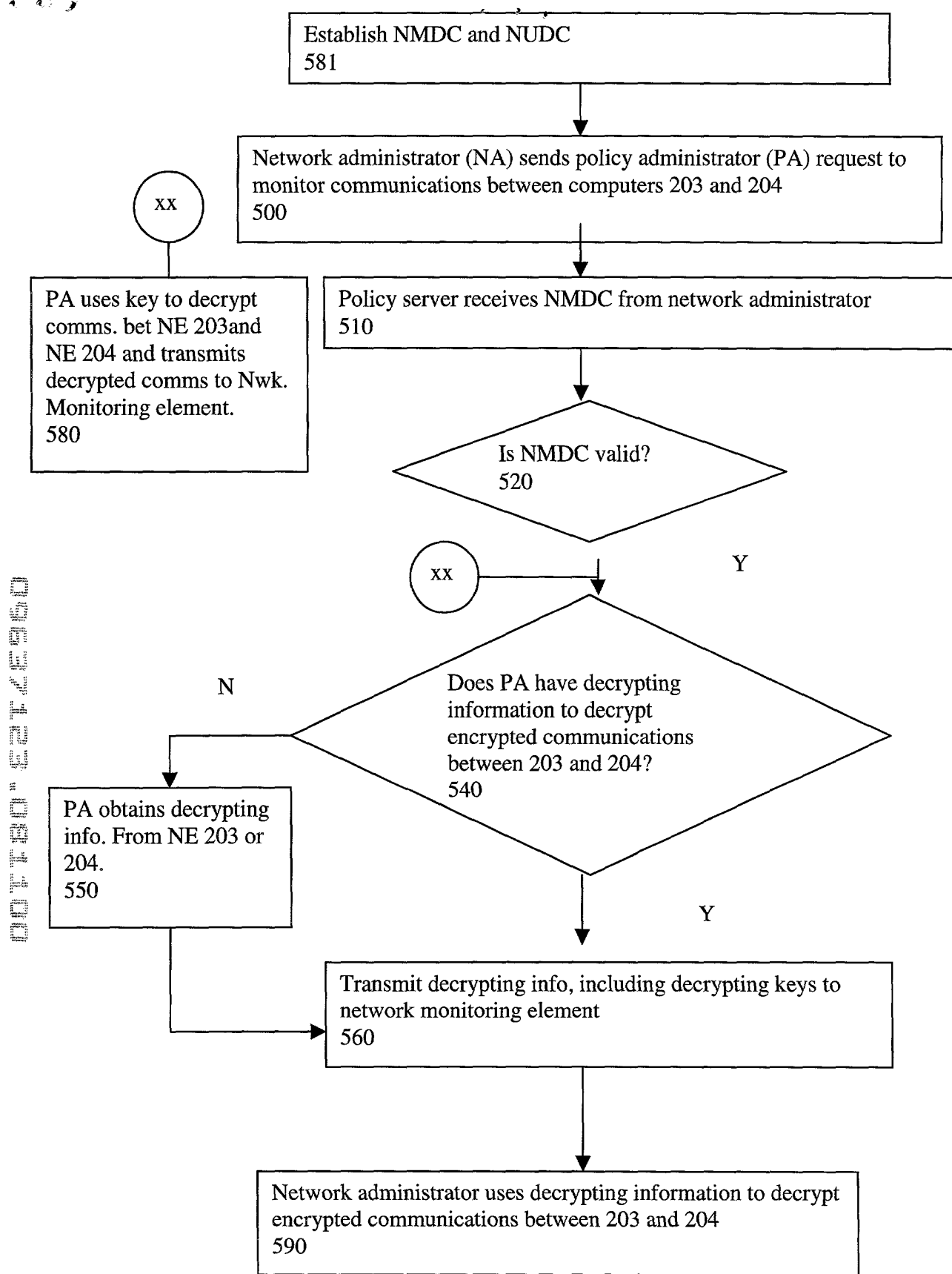


Figure 5

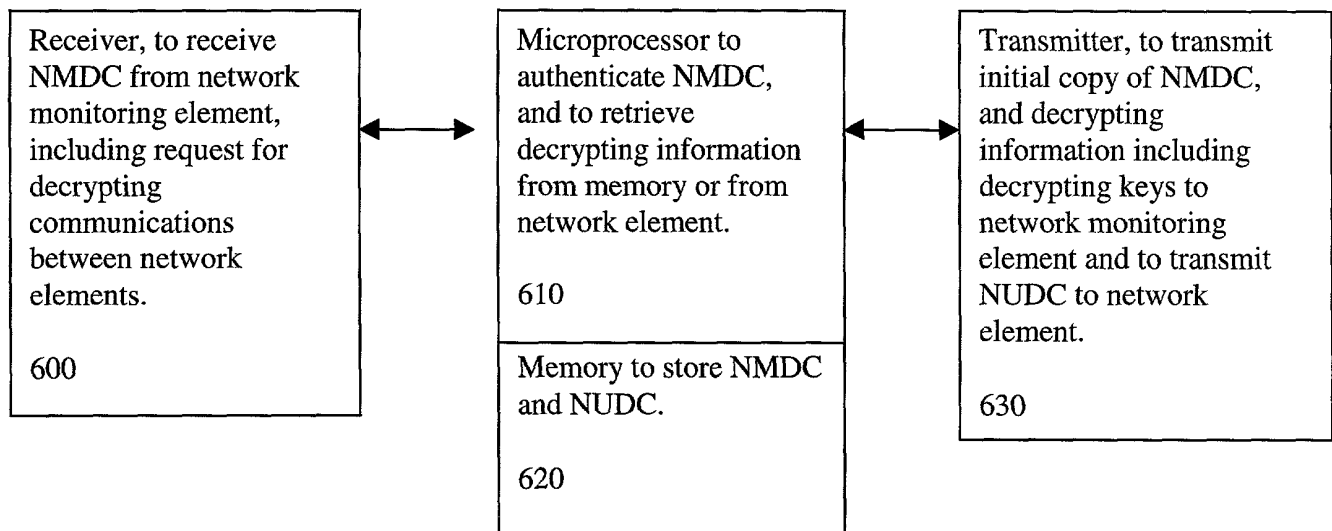


Figure. 6

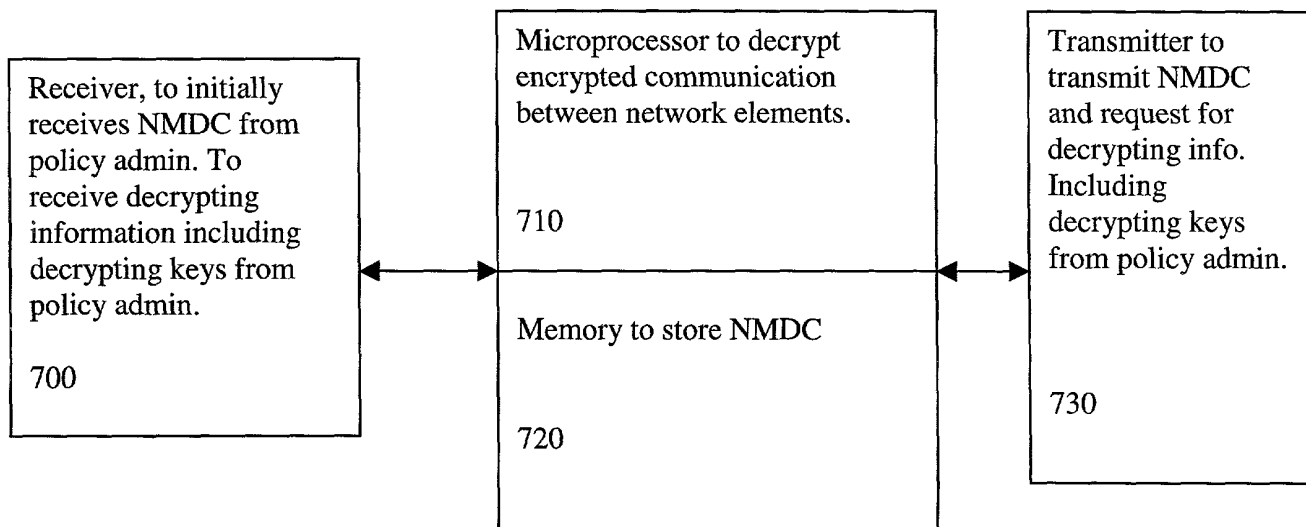


Figure 7

**DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION  
(FOR INTEL CORPORATION PATENT APPLICATIONS)**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

**METHOD AND APPARATUS FOR MONITORING ENCRYPTED COMMUNICATIONS  
IN A NETWORK**

the specification of which



is attached hereto.

was filed on \_\_\_\_\_ as \_\_\_\_\_

United States Application Number \_\_\_\_\_

or PCT International Application Number \_\_\_\_\_

and was amended on \_\_\_\_\_

(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, and that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):

APPLICATION NUMBER	COUNTRY (OR INDICATE IF PCT)	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 37 USC 119
			<input type="checkbox"/> No <input type="checkbox"/> Yes
			<input type="checkbox"/> No <input type="checkbox"/> Yes
			<input type="checkbox"/> No <input type="checkbox"/> Yes

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

APPLICATION NUMBER	FILING DATE

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION NUMBER	FILING DATE	STATUS (ISSUED, PENDING, ABANDONED)

I hereby appoint the persons listed on Appendix A hereto (which is incorporated by reference and a part of this document) as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to:

Clive D. Menezes, Reg. No. 45,493, BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

(Name of Attorney or Agent)

12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025 and direct telephone calls to:

Clive D. Menezes, (503) 684-6200.

(Name of Attorney or Agent)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor (given name, family name)

Ramanathan Ramanathan

Inventor's Signature

Ramanathan Ramanathan

Date

8/11/2000

Residence Portland, Oregon USA

(City, State)

Citizenship India

(Country)

P. O. Address 15414 N.W. Energia St.

Portland, Oregon 97229 USA

## APPENDIX A

William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. 42,261; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Lisa N. Benado, Reg. No. 39,995; Bradley J. Berezna, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; R. Alan Burnett, Reg. No. 46,149; Gregory D. Caldwell, Reg. No. 39,926; Andrew C. Chen, Reg. No. 43,544; Thomas M. Coester, Reg. No. 39,637; Donna Jo Coningsby, Reg. No. 41,684; Florin Corie, Reg. No. 46,244; Dennis M. deGuzman, Reg. No. 41,702; Stephen M. De Klerk, Reg. No. P46,503; Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Robert Andrew Diehl, Reg. No. 40,992; Sanjeet Dutta, Reg. No. P46,145; Matthew C. Fagan, Reg. No. 37,542; Tarek N. Fahmi, Reg. No. 41,402; George Fountain, Reg. No. 37,374; James Y. Go, Reg. No. 40,621; James A. Henry, Reg. No. 41,064; Willmore F. Holbrow III, Reg. No. P41,845; Sheryl Sue Holloway, Reg. No. 37,850; George W. Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; William W. Kidd, Reg. No. 31,772; Sang Hui Kim, Reg. No. 40,450; Walter T. Kim, Reg. No. 42,731; Eric T. King, Reg. No. 44,188; Jason K. Klindtworth, Reg. No. P47,211; Erica W. Kuo, Reg. No. 42,775; George B. Leavell, Reg. No. 45,436; Gordon R. Lindeen III, Reg. No. 33,192; Jan Carol Little, Reg. No. 41,181; Kurt P. Leyendecker, Reg. No. 42,799; Joseph Lutz, Reg. No. 43,765; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Clive D. Menezes, Reg. No. 45,493; Chun M. Ng, Reg. No. 36,878; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Daniel E. Ovanezian, Reg. No. 41,236; Kenneth B. Paley, Reg. No. 38,989; Marina Portnova, Reg. No. P45,750; William F. Ryann, Reg. 44,313; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Jeffrey Sam Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; John F. Travis, Reg. No. 43,203; Joseph A. Twarowski, Reg. No. 42,191; Thomas A. Van Zandt, Reg. No. 43,219; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Mark L. Watson, Reg. No. P46,322; Thomas C. Webster, Reg. No. P46,154; and Norman Zafman, Reg. No. 26,250; my patent attorneys, and Justin M. Dillon, Reg. No. 42,486; my patent agent, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (310) 207-3800, and Alan K. Aldous, Reg. No. 31,905; Robert D. Anderson, Reg. No. 33,826; Joseph R. Bond, Reg. No. 36,458; Richard C. Calderwood, Reg. No. 35,468; Jeffrey S. Draeger, Reg. No. 41,000; Cynthia Thomas Faatz, Reg. No. 39,973; Sean Fitzgerald, Reg. No. 32,027; John N. Greaves, Reg. No. 40,362; Seth Z. Kalson, Reg. No. 40,670; David J. Kaplan, Reg. No. 41,105; Charles A. Mirho, Reg. No. 41,199; Leo V. Novakoski, Reg. No. 37,198; Naomi Obinata, Reg. No. 39,320; Thomas C. Reynolds, Reg. No. 32,488; Kenneth M. Seddon, Reg. No. 43,105; Mark Seeley, Reg. No. 32,299; Steven P. Skabrat, Reg. No. 36,279; Howard A. Skaist, Reg. No. 36,008; Steven C. Stewart, Reg. No. 33,555; Raymond J. Werner, Reg. No. 34,752; Robert G. Winkle, Reg. No. 37,474; and Charles K. Young, Reg. No. 39,435; my patent attorneys, and Thomas Raleigh Lane, Reg. No. 42,781; Calvin E. Wells; Reg. No. P43,256, Peter Lam, Reg. No. 44,855; and Gene I. Su, Reg. No. 45,140; my patent agents, of INTEL CORPORATION; and James R. Thein, Reg. No. 31,710, my patent attorney; with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.